

Amendments to the Claims

This listing of claims will replace all prior versions, and listings, of claims in the application.

1-9. (Canceled)

10. (Currently Amended) A method for providing access ~~management to a~~ secured item, comprising:

authenticating a user to a ~~first and a second server machine, whereby the~~
~~first and the second server machines are configured to comprise a~~ having the
secured item stored therein;

preventing access to ~~[[the]] a second server machine~~ having the secured
item stored therein while the user is accessing the first server ~~machine through a~~
~~first connection from a first location~~; and

upon receiving an access request from the user to access the second server
~~machine from a second location~~, authenticating the user to the second server, and
disconnecting the user from the first ~~connection~~ server before establishing a
~~second connection~~ that allows the user to access the second server ~~machine~~.

11. (Currently Amended) The method as recited in claim ~~[[29]]~~ 10, wherein
the authenticating ~~[[the]] a~~ user comprises authenticating both the user and a client
machine being used by the user.

12. (Currently Amended) The method as recited in claim 10, wherein the
first and the second ~~server machines~~ servers are access points for the user to gain access
to the secured item.

Reply to Office Action of March 16, 2009

13. (Currently Amended) The method as recited in claim 29, wherein:

when the user is at [[a]] the first location, the user interacts over a network with the first server ~~machine~~, and

when the user is at [[a]] the second location, the user interacts over a network with the second server ~~machine~~ using a second client machine at the second location.

14. (Currently Amended) The method as recited in claim 10, ~~wherein the method further comprises~~ comprising:

determining, prior to disconnecting the user from the first ~~connection~~ server, whether the user is permitted to gain access through [[a]] the second location to the secured item via the second server ~~machine~~.

15. (Currently Amended) The method as recited in claim 29, wherein the authenticating the user with the first server occurs while the user is at [[a]] the first location, and wherein the receiving the access request occurs while the user is at [[a]] the second location.

16. (Currently Amended) The method as recited in claim 17, wherein the [[the]] authenticating the user to the second server further comprises:

upon receiving the access request to access the secured item via the second server ~~machine~~, determining permitted locations from which the user is permitted to access the secured item;

determining whether the second location is one of the permitted locations for the user; and

Reply to Office Action of March 16, 2009

bypassing the disconnecting the user from the first ~~connection~~
server in response to the determination that the second location is not one of the
permitted locations for the user.

17. (Currently Amended) The method as recited in claim 30, wherein:
when the user is at [[a]] the first location, the user interacts over a network
with the first server ~~machine~~ using a first client machine at the first location, and
when the user is at [[a]] the second location, the user interacts over a
network with the second server ~~machine~~ using a second client machine at the
second location.

18. (Currently Amended) A ~~computer-readable~~ tangible computer-readable
medium ~~containing~~ having stored thereon, computer-executable instructions for
~~controlling at least one processor by that, if executed by a computing device, cause the~~
computing device to perform a method, comprising:

authenticating a user to a first ~~and a second~~ server ~~machine~~, whereby the
~~first and the second server machines are configured to comprise~~ having a secured
item stored therein;

preventing access to [[the]] a second server ~~machine~~ having the secured
item stored therein while the user is accessing the first server ~~machine through a~~
~~first connection from a first location~~; and

upon receiving an access request from the user to access the second server
~~machine from a second location~~, authenticating the user to the second server, and
disconnecting the user from the first ~~connection~~ server before establishing a
~~second~~ connection that allows the user to access the second server ~~machine~~.

19. (Currently Amended) The ~~computer-readable~~ tangible computer-readable medium as recited in claim 31, wherein:

when the user is at [[a]] the first location, the user interacts over a network with the first server ~~machine~~, and

when the user is at [[a]] the second location, the user interacts over a network with the second server ~~machine~~ using a second client machine at the second location.

20. (Currently Amended) The ~~computer-readable~~ tangible computer-readable medium as recited in claim 32, further comprising:

determining, prior to the reconfiguring of either the first local module at the first server ~~machine~~ or the second local module at the second server ~~machine~~, whether the user is permitted to gain access from [[a]] the second location to the secured item via the second server ~~machine~~.

21. (Currently Amended) A system for ~~providing~~ controlling access management to a secured item, comprising:

an access control device, wherein the access control device authenticates a user to a first ~~and a second~~ server ~~machine~~, whereby the first ~~and the second~~ server ~~machines are configured to comprise a~~ having the secured item stored therein, and prevents access to [[the]] a second server machine while the user is accessing the first server ~~machine through a first connection~~ from a first location, and, upon receiving an access request from the user to access the second server ~~machine from a second location~~, authenticates the user to the second server, and

Reply to Office Action of March 16, 2009

disconnects the user from the first ~~connection~~ server before establishing a ~~second~~ connection that allows the user to access the second server ~~machine~~.

22. (Currently Amended) The ~~computer-readable~~ tangible computer-readable medium as recited in claim 31, wherein authenticating ~~[[a]]~~ the user comprises authenticating both the user and a client machine being used by the user.

23. (Currently Amended) The ~~computer-readable~~ tangible computer-readable medium as recited in claim 32, further comprising:

determining, prior to the reconfiguring the first local module at the first server ~~machine~~ and the second local module at the second server ~~machine~~, whether the user is permitted to gain access from ~~[[a]]~~ the second location to the secured item via the second server ~~machine~~.

24. (Currently Amended) The ~~computer-readable~~ tangible computer-readable medium as recited in claim 33, wherein the authenticating the user to the second server further comprises:

upon receiving the access request to access the secured item via the second server ~~machine~~, determining permitted locations from which the user is permitted to gain access to the secured item;

determining whether the second location is one of the permitted locations for the user; and

bypassing the disconnecting the user from the first ~~connection~~ server in response to the determination that the second location is not one of the permitted locations for the user.

25. (Previously Presented) The system as recited in claim 21, wherein the access control device authenticates both the user and a client machine being used by the user.

26. (Currently Amended) The system as recited in claim 21, wherein the first and the second ~~server machines~~ servers are access points for the user to gain access to the secured item.

27. (Currently Amended) The system as recited in claim 35, wherein the access control device determines, prior to reconfiguring the first local module at the first server ~~machine~~ and the second local module at the second server ~~machine~~, whether the user is permitted to gain access from [[a]] the second location to the secured item via the second server ~~machine~~.

28. (Canceled)

29. (Currently Amended) The method as recited in claim 10, ~~wherein the authenticating the user comprises~~ further comprising:

authenticating the user with the first server ~~machine~~ with respect to a previous access request;

subsequently receiving the access request via the second server ~~machine~~;

and

authenticating the user with the second server ~~machine~~ with respect to the access request.

Reply to Office Action of March 16, 2009

30. (Currently Amended) The method as recited in claim 29, wherein the disconnecting the user from the first ~~connection~~ server comprises:

upon receiving the access request via the second server ~~machine~~,
identifying a first local module previously supporting the user at the first server
~~machine~~;

reconfiguring the first local module at the first server ~~machine~~ to remove
support for the user at the first server ~~machine~~;

identifying a second local module to support the user at the second server
~~machine~~; and

reconfiguring the second local module at the second server ~~machine~~ to
add support for the user at the second server ~~machine~~.

31. (Currently Amended) The ~~computer-readable~~ tangible computer-readable
medium as recited in claim 18, ~~wherein the authenticating the user comprises~~ further
comprising:

authenticating the user with the first server ~~machine~~ with respect to a
previous access request;

subsequently receiving the access request via the second server ~~machine~~;
and

authenticating the user with the second server ~~machine~~ with respect to the
access request.

32. (Currently Amended) The ~~computer-readable~~ tangible computer-readable
medium as recited in claim 31, wherein the disconnecting the user from the first
~~connection~~ server comprises:

Reply to Office Action of March 16, 2009

upon receiving the access request via the second server ~~machine~~,
identifying a first local module previously supporting the user at the first server
~~machine~~;

reconfiguring the first local module at the first server ~~machine~~ to remove
support for the user at the first server ~~machine~~;

identifying a second local module to support the user at the second server
~~machine~~; and

reconfiguring the second local module at the second server ~~machine~~ to
add support for the user at the second server ~~machine~~.

33. (Currently Amended) The ~~computer-readable~~ tangible computer-readable
medium as recited in claim 32, wherein:

when the user is at ~~[[a]]~~ the first location, the user interacts over a network
with the first server ~~machine~~ using a first client machine at the first location, and

when the user is at ~~[[a]]~~ the second location, the user interacts over a
network with the second server ~~machine~~ using a second client machine at the
second location.

34. (Currently Amended) The system as recited in claim 21, wherein the
access control device:

authenticates the user with the first server ~~machine~~ with respect to a
previous access request;

subsequently receives the access request via the second server ~~machine~~;
and

Reply to Office Action of March 16, 2009

authenticates the user with the second server ~~maehine~~ with respect to the access request.

35. (Currently Amended) The system as recited in claim 34, wherein the access control device:

identifies a first local module previously supporting the user at the first server ~~machine~~ upon receiving the access request to access the secure item via the second server ~~machine~~;

reconfigures the first local module at the first server ~~machine~~ to remove support for the user at the first server ~~machine~~;

identifies a second local module to support the user at the second server ~~machine~~; and

reconfigures the second local module at the second server ~~machine~~ to add support for the user at the second server ~~machine~~.